17feb06 15:29:01 User259284 Session D3498.2

File 256:TecInfoSource 82-2006/Feb

Set	Items	Description
S1	1197	FIREWALL??
S2	0	FIRE()WALL?????
S3	1200	FIREWALL??????
S4	10	S3 AND DELAY?????
S5	1	S3 AND DURATION????
S6	0	S3 AND ELAPS???????
S7	338	S3 AND (CLOCK????? OR JITTER????? OR TIME?????? OR TIMING?-??? OR SPEED????)
S8	27	FIREWALL?????(5N)(CLOCK????? OR JITTER????? OR TIME?????? -OR TIMING???? OR SPEED????)
S9	174	S1 AND PORT????
S10	57	S1 AND (ACROSS OR THROUGH)(2N)FIREWALL?????
S11	665	S1 AND (MEASUR???????? OR MONITOR????? OR SENS??? OR DETEC-T?????? OR DETERMIN?????? OR PRESELECT?????? OR PREDETERMIN??-?????)
S12	83	S1 AND (PRE()SELECT?????? OR PRE()DETERMIN??????? OR TARGE-T???? OR GOAL??)
S13	4	S1 AND DESIRED
S14	7	S1 AND CALCULAT???????
S15	2	S1 AND PRESET????
S16	0	S1 AND PRE()SET????
S17	191	S1 AND (WARN??????? OR NOTIF??????? OR ALERT?????? OR ALAR-M??????? OR ANNOUN?????? OR ANNUNC?????)
S18	418	S1 AND ENTER????????
S19	0	S1 AND INLET??????
S20	31	S1 AND INCOM???????
S21	42	S1 AND ALLOWING
S22	23	S1 AND ALLOWED
S23	247	S1 AND ALLOWS
S24	14	S1 AND PERMITTING
S25	15	S1 AND PERMITTED
S26	5	S1 AND THRESHOLD?
S27	0	S1 AND THRESHHOLD?
S28	17	S1 AND LIMIT
S29	26	S1 AND RESTRICT????????
S30	13	S1 AND (COMPLIE??? OR COMPLIANT OR COMPLIANCE?? OR COMPLY?-??? OR COMPATIB????????)(5N)(STANDARD???? OR RFC OR COMMENT? ? OR SPECIFICATION?? OR REQUIREMENTS)
S31	2	S1 AND (COMPLIE??? OR COMPLIANT OR COMPLIANCE?? OR COMPLY?-??? OR COMPATIB????????)(5N)INDUSTR?????
S32	1	S1 AND (COMPLIE??? OR COMPLIANT OR COMPLIANCE?? OR COMPLY?-??? OR COMPATIB????????)(5N)(VOIP OR PROROCOL???)
S33	344	S4:S8
S34	51	9AND33
S35	22	S10 AND S32:S34
S36	4	S35 AND (OPEN????? OR CLOSE OR CLOSED OR CLOSES OR CLOSING-?? OR SHUT??????)
S37	30	(PORT OR PORTS)(4N)(CLOS????? OR OPEN OR OPENS OR OPENED OR OPENING??)
S38	5	(PORT OR PORTS)(4N)SHUT??????
S39	27	(PORT OR PORTS)(4N)USED
S40	20	(PORT OR PORTS)(4N)USE
S41	11	(PORT OR PORTS)(4N)USING
S42	0	(PORT OR PORTS)(4N)UTILIS?

```
S43          4   (PORT OR PORTS)(4N)UTILIZ?
S44         91   S37:S43
S45         32   3AND44
S46         32   S45 AND S4:S35
S47          0   S46 AND THRESHHOLD?
S48          0   S46 AND THRESHOLD?
S49          0   S46 AND (COMPLIE??? OR COMPLIANT OR COMPLIANCE?? OR COMPLY-
                 ???? OR COMPATIB????????)(5N)(VOIP OR PROTOCOL???)
S50          0   S46 AND (COMPLIE??? OR COMPLIANT OR COMPLIANCE?? OR COMPLY-
                 ???? OR COMPATIB????????)(5N)INDUSTR?????
S51          6   S46 AND (WARN??????? OR NOTIF??????? OR ALERT?????? OR ALA-
                 RM??????? OR ANNOUN?????? OR ANNUNC?????)
S52          6   S51 NOT S36
S53        418   S4:S5 OR S8 OR S10 OR S12:S15 OR S20:S22 OR S24:S32 OR S34-
                 :S46
S54        359   S53 AND FIREWALL???????
S55         16   S54 AND DYNAMIC????????
S56          1   S54 AND VERIZON??????
S57         70   S54 AND (PORT OR PORTS)
S58         89   (MONITOR???? OR SENS??? OR DETECT????? OR DELAY??????)(4N)-
                 (OPEN????? OR CLOSE OR CLOSED OR CLOSES OR CLOSING?? OR SHUT?-
                 ?????)
S59          5   (MONITOR???? OR SENS??? OR DETECT?????)(4N)DELAY?????
S60          4   (MONITOR???? OR SENS??? OR DETECT?????)(4N)(LAG OR LAGS OR
                 LAGG???? OR SLOW?????)
S61         98   S58:S60
S62          6   S61 AND (PORT OR PORTS)
S63          9   S61 AND FIREWALL?????????
S64          3   55AND57
S65          0   55AND58
S66          1   57AND58
S67         60   S5 OR S13:S15 OR S26 OR S31:S32 OR S36 OR S38 OR S43 OR S56
                 OR S59:S60 OR S62:S66
S68         40   S67 AND FIREWALL???????
S69         36   S68 NOT (S52 OR S36)
S70          8   S69 AND (PORT OR PORTS)
S71         25   BLUESOCKET?
S72          4   S71 AND FIREWALL?????????
S73          3   S72 NOT (S70 OR S52 OR S36)
S74         36   FIREWALL??????? AND (WARN??????? OR NOTIF??????? OR ALERT?-
                 ????? OR ALARM??????? OR ANNOUN?????? OR ANNUNC?????)(7N)(PORT
                 OR PORTS OR FIREWALL?????????)
S75         35   S74 NOT (S70 OR S73 OR S52 OR S36)
S76         15   S75 AND (CLOCK????? OR JITTER????? OR TIME?????? OR TIMING-
                 ???? OR SPEED???? OR DELAY??????? OR DURATION?? OR LAPS????? -
                 OR LAG?? OR LAGG??????)
S77         15   S75 AND (WARN??????? OR NOTIF??????? OR ALERT?????? OR ALA-
                 RM??????? OR ANNOUN?????? OR ANNUNC?????)(3N)(PORT OR PORTS OR
                 FIREWALL?????????)
S78         24   S76:S77
S79          6   76AND77
S80         13   DYNAMIC???????(5N)(PORT OR PORTS OR FIREWALL???????)
S81          7   FIREWALL??????? AND S80
S82          4   S81 NOT (S79 OR S70 OR S73 OR S52 OR S36)
```

17feb06 16:39:19 User259284 Session D3498.5

SYSTEM:OS - DIALOG OneSearch
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200611
(c) 2006 Thomson Derwent
*File 350: For more current information, include File 331 in your search.
Enter HELP NEWS 331 for details.
File 347:JAPIO Nov 1976-2005/Oct(Updated 060203)
(c) 2006 JPO & JAPIO
File 344:Chinese Patents Abs Jan 1985-2006/Jan
(c) 2006 European Patent Office
File 348:EUROPEAN PATENTS 1978-2006/Feb W02
(c) 2006 European Patent Office
*File 348: For important information about IPCR/8 and forthcoming
changes to the IC= index, see HELP NEWSIPCR.
File 349:PCT FULLTEXT 1979-2006/UB=20060209,UT=20060202
(c) 2006 WIPO/Univentio

Set	Items	Description
S1	4	FIREWALL????(8N)(DELAY?????)(8N)(ALERT???? OR ALARM????)
S2	666	FIREWALL????(8N)(PORT OR PORTS)
S3	3211	DELAY?????(8N)(PORT OR PORTS)
S4	1180	(ALERT???? OR ALARM????)(8N)(PORT OR PORTS)
S5	1	1AND2
S6	2	1AND3
S7	1	1AND4
S8	2	S5:S7
S9	44	FIREWALL????(8N)(DELAY?????)
S10	85	FIREWALL????(8N)(ALERT???? OR ALARM????)
S11	666	FIREWALL????(8N)(PORT OR PORTS)
S12	1	2AND3AND4
S13	2	9AND10AND11
S14	1	S12:S13 NOT S8
S15	41	DYNAMIC?????(3N)FIREWALL?????/TI,AB,CM
S16	7	2AND15
S17	0	3AND15
S18	0	4AND15
S19	2	9AND15
S20	2	10AND15
S21	7	11AND15
S22	13	S1 OR S16:S21
S23	11	S22 NOT (S12 OR S13 OR S8)
S24	7	S23 AND (PORT OR PORTS)/TI,AB,CM
S25	3	S23 AND DELAY???????/TI,AB,CM
S26	4	S23 AND (ALARM???? OR ALERT???? OR WARNING??)/TI,AB,CM
S27	10	S23 AND (FIREWALL?????)/TI,AB,CM
S28	2	24AND25
S29	2	24AND26
S30	7	24AND27
S31	2	S28:S29
S32	2	30AND31
S33	9	S23:S31 NOT S32
S34	3	S33 AND (PORT OR PORTS)/TI,AB
S35	6	S33 NOT S34

---------- 2/17/06 10/678,779

17feb06 16:18:30 User259284 Session D3498.4

SYSTEM:OS - DIALOG OneSearch
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200611
(c) 2006 Thomson Derwent
*File 350: For more current information, include File 331 in your search.
Enter HELP NEWS 331 for details.
File 347:JAPIO Nov 1976-2005/Oct(Updated 060203)
(c) 2006 JPO & JAPIO
File 344:Chinese Patents Abs Jan 1985-2006/Jan
(c) 2006 European Patent Office
File 23:CSA Technology Research Database 1963-2006/Jan
(c) 2006 CSA.
File 2:INSPEC 1898-2006/Jan W4
(c) 2006 Institution of Electrical Engineers
*File 2: Archive data back to 1898 has been added to File 2.
File 6:NTIS 1964-2006/Feb W1
(c) 2006 NTIS, Intl Cpyrght All Rights Res
File 8:Ei Compendex(R) 1970-2006/Feb W1
(c) 2006 Elsevier Eng. Info. Inc.
File 14:Mechanical and Transport Engineer Abstract 1966-2006/Jan
(c) 2006 CSA.
File 25:Weldasearch-19662006/Jan (c) 2006 TWI Ltd
File 31:World Surface Coatings Abs 1976-2006/Feb
(c) 2006 PRA Coat. Tech. Cen.
File 33:Aluminium Industry Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 34:SciSearch(R) Cited Ref Sci 1990-2006/Feb W2
(c) 2006 Inst for Sci Info
File 35:Dissertation Abs Online 1861-2006/Jan
(c) 2006 ProQuest Info&Learning
File 36:MetalBase 1965-20060215
(c) 2006 The Dialog Corporation
File 46:Corrosion Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 56:Computer and Information Systems Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 57:Electronics & Communications Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 60:ANTE: Abstracts in New Tech & Engineer 1966-2006/Jan
(c) 2006 CSA.
File 61:Civil Engineering Abstracts. 1966-2006/Jan
(c) 2006 CSA.
File 63:Transport Res(TRIS) 1970-2006/Jan
(c) fmt only 2006 Dialog
File 64:Environmental Engineering Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 65:Inside Conferences 1993-2006/Feb W2
(c) 2006 BLDSC all rts. reserv.
File 68:Solid State & Superconductivity Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 81:MIRA - Motor Industry Research 2001-2006/Dec
(c) 2006 MIRA Ltd.
File 94:JICST-EPlus 1985-2006/Nov W4
(c)2006 Japan Science and Tech Corp(JST)
File 95:TEME-Technology & Management 1989-2006/Feb W2
(c) 2006 FIZ TECHNIK
File 96:FLUIDEX 1972-2006/Feb
(c) 2006 Elsevier Science Ltd.
File 99:Wilson Appl. Sci & Tech Abs 1983-2006/Jan
(c) 2006 The HW Wilson Co.

---------- 2/17/06 10/678,779

File 103:Energy SciTec 1974-2006/Jan B2
(c) 2006 Contains copyrighted material
*File 103: For access restrictions see Help Restrict.
File 104:AeroBase 1999-2006/Jan
(c) 2006 Contains copyrighted material
File 118:ICONDA-Intl Construction 1976-2006/Jan
(c) 2006 Fraunhofer-IRB
File 134:Earthquake Engineering Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 144:Pascal 1973-2006/Jan W4
(c) 2006 INIST/CNRS
File 239:Mathsci 1940-2006/Mar
(c) 2006 American Mathematical Society
File 240:PAPERCHEM 1967-2006/Feb W2
(c) 2006 Elsevier Eng. Info. Inc.
File 248:PIRA 1975-2006/Jan W4
(c) 2006 Pira International
File 293:Engineered Materials Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 315:ChemEng & Biotec Abs 1970-2005/Dec
(c) 2005 DECHEMA
File 323:RAPRA Rubber & Plastics 1972-2006/Jan
(c) 2006 RAPRA Technology Ltd
*File 323: Alert feature enhanced for multiple files, duplicate removal, customized scheduling. See HELP ALERT.
File 335:Ceramic Abstracts/World Ceramics Abstracts 1966-2006/Jan
(c) 2006 CSA.
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info

Set	Items	Description
S1	5	FIREWALL???????/TI AND DELAY??????/TI
S2	2616	FIREWALL????/TI
S3	166	S2 AND (PORT OR PORTS)
S4	76	S2 AND (ALERT????? OR ALARM????? OR WARN????? OR NOTIF????-???)
S5	9	3AND4
S6	13	S1 OR S5
S7	12	RD S6 (unique items)

17feb06 16:01:57 User259284 Session D3498.3

Set	Items	Description
S1	29340	PORT OR PORTS
S2	2152	'FIREWALLS' OR FIREWALL?????? OR FIRE()WALL????? OR ('AUTHORISATION' AND 'COMPUTER NETWORKS')
S3	372	('AUTHORISATION' AND 'COMPUTER NETWORKS')
S4	2152	S2:S3
S5	76	S1 AND S4
S6	14	S5 AND DYNAMIC?
S7	2	ALARM?????? AND S5
S8	172	S4 AND ('ALARM SYSTEMS' OR 'WARNING SYSTEMS' OR 'INDICATORS' OR 'MONITORING' OR 'SENSORS' OR 'SIGNALLING' OR CC='D3035')
S9	2	6AND8
S10	1	S9 NOT S7
S11	19	S4 AND R1:R7
S12	22	S4 AND R1:R12
S13	11	11AND12
S14	11	S13 NOT (S9 OR S7)
S15	1705	DELAY?????(7N)(OPEN????? OR CLOSE OR CLOSED OR CLOSING?? OR SHUT??????)
S16	0	4AND15
S17	3	S5 AND DELAY???????
S18	14	S5 AND (OPEN????? OR CLOSE OR CLOSED OR CLOSING?? OR SHUT?????)
S19	15	S17:S18 NOT (S14 OR S10 OR S7)
S20	15	(S3 OR S5:S14) AND S19
S21	15	2AND20
S22	15	1AND20
S23	67290	R1:R10
S24	298787	R1:R10
S25	314247	S23:S24
S26	999	1AND25
S27	69	2AND25
S28	15	3AND25
S29	7	8AND25
S30	4	26AND27
S31	0	26AND28
S32	0	26AND29
S33	15	27AND28
S34	7	27AND29
S35	24	S28:S34
S36	20	S35 NOT (S14 OR S10 OR S7 OR S22)
S37	3	S36 AND (DELAY??????? OR ALARM???????? OR ALERT??????)
S38	17	S36 NOT S37
S39	3	S38/2004-2006
S40	14	S38 NOT S39
S41	1	S40 AND (PORT OR PORTS)
S42	0	FIREWALL???????/TI AND (PORT OR PORTS)/TI
S43	1	FIREWALL???????/TI AND DELAY??????/TI

SCIRUS
for scientific information only

"session control signalling" port Search

☑ Journal sources ☑ Preferred Web sources ☑ Other Web sources ☑ Exact phrase

Searched for:: :The exact phrase:**"session control signalling"** AND **port**

Found:: :**13 total | 0 journal results | 1 preferred web results | 12 other web results**

Sort by:: :**relevance** | **date**

Save checked results | Email checked results | Export checked results

1. SP-010714.doc [PDF-794K]
Dec 2001
Technical Specification Group Services and System Aspects TSGS#14(01)0714 Meeting #14, Kyoto, Japan, 17-20 December 2001 Source: TSG SA WG2 Title: CRs on 23.228 v.5.2.0 Agenda Item: 7.2.
more hits from [http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_14/Docs/PDF...]
similar results

2. The Essential Report on IP Telephony [PDF-417K]
Mar 2004
Today, we are pleased that the two camps are getting closer, and many difficult questions have been raised and answered. BDT's roles of catalyst and as a vehicle for information dissemination are essential to address issues of this nature, and we will continue to do so in the future.
[http://www.itu.int/itudoc/gs/promo/bdt/e-strat/85555.p...]
similar results

3. The Essential Report on IP Telephony [PDF-417K]
May 2004
Today, we are pleased that the two camps are getting closer, and many difficult questions have been raised and answered. BDT's roles of catalyst and as a vehicle for information dissemination are essential to address issues of this nature, and we will continue to do so in the future.
[http://uazuay.edu.ec/bibliotecas/mbaTI/uit/UIT%20The%2...]
similar results

4. Towards Interoperable Multimedia [PDF-35K]
May 2002
...server and client during a multimedia streaming **session**: **control/signalling** information and multimedia data. We describe...versions of RealSystem [9], and 3 Client Server 2n+1 **port** 2n **port** TCP-Control channel UDP-Data Channel UDP - Data...
[http://viola.usc.edu/paper/PV2002/86-iahangaell.pdf]
similar results

5. PERFORMANCE MANAGEMENT OF CELLULAR MOBILE PACKET DATA NETWORKS
MALOMSOKY, Szabolcs / VERES, Andrá / s / SZABÓ / , Istvá / n / BORSOS, Tamá / (...) / TELEFONAKTIEBOLAGET LM ERICSSON (publ), *PATENT COOPERATION TREATY APPLICATION*, Apr 2005
...Itsource IP address, destination IP address, source **port**, destination **port**&gt fields in the IP header and by looking up the &lsqb...with Mobility Database 106. Looking for the

Refine your search using these keywor found in the results
authorisation
bearer
charging
destination address
information flow
information flows
interoperability
network configuration
registration procedure
ringing
terminating
Or refine using:
All of the words
Refine

SCIRUS
for scientific information only

"session control signal" Search

Journal sources Preferred Web sources Other Web sources Exact phrase

Searched for:: :The exact phrase:**"session control signal"**

Found:: :**3 total | 0 journal results | 3 preferred web results | 0 other web results**

Sort by:: :**relevance | date**

Save checked results | Email checked results | Export checked results

Or refine using:
All of the words
Refine

1. METHOD AND SYSTEM FOR FACILITATING SERVICES IN A COMMUNICATION NETWORK THROUGH DATA-PUBLICATION BY A SIGNALING SERVER
McCONNELL, Von, K. / SANTHARAM, Arun / SPRINT SPECTRUM, L.P., *PATENT COOPERATION TREATY APPLICATION*, Aug 2003
A mechanism is disclosed for facilitating the performance of communication services in a communication network. An enhanced proxy server (14) receives a signaling message and proxies the message to an application server (16). Further, the enhanced...
Full text available at patent office. For more in-depth searching go to LexisNexis
view all 3 results from Patent Offices
similar results

2. Simultaneous over the air data download to multiple radios
Doiron, Timothy J. / Dreon, Steven T. / Ericsson, Inc., *UNITED STATES PATENT AND TRADEMARK OFFICE GRANTED PATENT*, Oct 2000
...requests an acknowledgment, which is returned one- by-one from each mobile radio. Finally, a disconnect broadcast **session control signal** is then repetitiously broadcast to the radios.
Full text available at patent office. For more in-depth searching go to LexisNexis
view all 3 results from Patent Offices
similar results

3. SERVICE SESSION CONTROLLER
ISHIZUKA MASARU / OKI ELECTRIC IND CO LTD, *PATENT ABSTRACTS OF JAPAN*, Mar 1999
...performs control in decentralized OS environment, the service session gateway 6 converts a **session control signal** from the client 2 into a **session control signal** of the decentralized OS environment 7 based upon the decentralized environment.
Full text available at patent office. For more in-depth searching go to LexisNexis
view all 3 results from Patent Offices
similar results

7/9/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

- Same applicant
- Different Case

016989045
WPI Acc No: 2005-313359/200532
XRPX Acc No: N05-256084

Firewall testing method for use in voice over Internet protocol network, involves determining port opening and closing **delays** from time of transmitted signal, when terminating established communication session

Patent Assignee: HARVEY E P (HARV-I); ORMAZABAL G S (ORMA-I); SYLVESTER J E (SYLV-I)
Inventor: HARVEY E P; ORMAZABAL G S; SYLVESTER J E

Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20050076238	A1	20050407	US 2003679222	A	20031003	200532 B

Priority Applications (No Type Date): US 2003679222 A 20031003
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20050076238	A1		25	H04L-009/00	

Abstract (Basic): US 20050076238 A1

NOVELTY - The method involves sending a session initiation signal to initiate a communication session through a firewall and a session termination signal to terminate an established communication session. A port opening delay and a port closing delay that occur in regard to opening and closing a port in the firewall are determined from the time of transmitted signal, when terminating an established communications session.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a firewall test apparatus.

USE - Used for testing a firewall in a voice over Internet protocol network.

ADVANTAGE - The occurrence of the port opening and closing delays are determined from time of transmitted signal, when terminating established communication session, thus facilitating strict verification of security measures employed in voice over Internet protocol (VoIP) network.

DESCRIPTION OF DRAWING(S) - The drawing shows a flow chart illustrating steps of a firewall test method.

pp; 25 DwgNo 5B/9

Title Terms: FIREWALL; TEST; METHOD; VOICE; PROTOCOL; NETWORK; DETERMINE; PORT; OPEN; CLOSE; DELAY; TIME; TRANSMIT; SIGNAL; TERMINATE; ESTABLISH; COMMUNICATE; SESSION
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00
File Segment: EPI
Manual Codes (EPI/S-X): T01-N01D1A; T01-N02B1D; W01-A05A; W01-C05B4C

70/9/8
DIALOG(R)File 256:TecInfoSource

00141008 DOCUMENT TYPE: Review

PRODUCT NAMES: VoIP (837067); **Firewalls** (837661

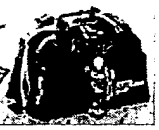
TITLE: VOIP vs. **Firewalls**
AUTHOR: Krapf, Eric
SOURCE: Business Communications Review, v32 n7 p10(1) **Jul 2002**
ISSN: 0162-3885
HOMEPAGE: http://www.bcr.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

New solutions are becoming available from such **firewall** vendors as Cisco, Check Point, Aravox, and Ingate that allow **dynamic port opening** on their devices. Most support H.323 and SIP (Session Initiation Protocol). **Dynamic port opening** can affect performance because it will add **delay** and **jitter**, which impact Voice-over-IP (VoIP) adversely. The tools are meant to protect the network from attack by only **opening** VoIP **ports** when traffic has to get through and shutting them when the call is torn down. A spokesperson for Check Point says performance is not an issue, even for Check Point's software-based **firewalls**. On some appliances, Check Point gets 3Gbps of throughput, which is sufficient. However, **opening** a **port** also means updating the **firewall**'s policy, and there is not much of a **time** window do so. Andrew Molitor, chief scientist and co-founder of Aravox, says that in VoIP, voice packets follow swiftly after control packets, and a policy change request has only a few milliseconds to be completed once packets start to arrive. Another complicating factor is the number of concurrent policy updates that have to be handled during peak hours. More coordination and cooperation will also be required between those responsible for voice and those who do network security.

COMPANY NAME: TecTerms (999999)
SPECIAL FEATURE: Charts
DESCRIPTORS: Computer Security; **Firewalls**; Internet Security; Internetworking; Network Administration; Network Software; System **Monitoring**; VoIP
REVISION DATE: 20021230

BUSINESS COMMUNICATIONS REVIEW®



Current Articles
Older Articles

SUBSCRIBE NOW!
Subscriber Services
(Change of Address, etc.)

BCR eWeekly:
Free weekly enewsletter
your email
Subscribe
Read it in the BCR eForum

Search... Go
BCR Acronym Guide

JULY 2002 ISSUE:
- Voice Services Pricing: How Low *Can* They Go?

IN BRIEF:
- VOIP vs. Firewalls
- Outsourcing Trends in Uncertain Times
- Survey: VOIP Moves Beyond Cost-Cutting
- Web-Enabled Call Centers— A Progress Report
- Migrating Customers to Self-Service
- A Tale of Two Decisions
- Frame Relay: Good for Another 10 Years?

REVIEW:
- Avaya's CRM Enhancements

OPINION:
- Understanding How Users View Application Performance
- VOIP "Hype" Gap Slowly Closing
- The RBOCs: Why We Fight

TECHtionary
the animated technical dictionary

BCR White Papers
Search for White Papers and Analyst Research:
Go
Search Help
Advanced Search

BRIEFING

VOIP vs. Firewalls

from the July 2002 issue of Business Communications Review, p. 10

by Eric Krapf, managing editor of Business Communications Review

Enabling voice over IP (VOIP) to pass through a corporate firewall without endangering network security is shaping up to be a major challenge. Most of the firewalls installed today require network managers to open up yawning gaps in the firewall if VOIP is to get through, and while new solutions are emerging, they present their own problems.

Opening Ports

Firewalls protect a local or campus network by blocking incoming traffic based on application port numbers. The standard approach is to close all ports except those the enterprise specifically needs to keep open—e.g., for HTTP (Web) traffic. In legacy firewalls, open ports can only be closed via manual configuration.

But if you want to let VOIP traffic move from a public IP network onto your premises, you have to leave lots of ports open, explained Gary Audin, president of consultancy Delphi, Inc. For each voice conversation, two TCP or UDP ports have to be opened to allow H.323 or Session Initiation Protocol (SIP) signaling—one port for each direction. Then, for the voice traffic itself, two UDP ports must be opened and, optionally, two more UDP ports may be opened for Real-Time Control Protocol (RTCP), which monitors performance.

The VOIP ports run in sequences starting with Port 1024, which is a talk port, then 1025 to monitor 1024, then Port 1026 to listen, 1027 to monitor 1026, and so on, Audin explained.

Note that 2-4 UDP ports must be open for the duration of each call. If you need to support more than one simultaneous phone call, you'll have to open up a pool of many more ports. "You can create a blocking environment at your firewall if you run out of ports that are in your pool," Audin said.

And of course, the more ports you open up, the more you expose your internal network to attack. The solution that firewall vendors have hit on is to enable VOIP ports to be kept closed, then opened dynamically when traffic needs to get through, and closed once the call is torn down. This requires the firewall to understand enough of the VOIP call control to know which ports each call will use.

Dynamic Port Opening

Several firewall vendors, including Cisco, Check Point, Aravox and Ingate, enable dynamic port opening on their devices. Most support both H.323, the control protocol that's most common today, as well as SIP, which is expected to dominate eventually.

The natural concern in dynamic port opening is performance. Audin believes the negotiation process for dynamically opening ports will add delay and produce jitter, both of which can be serious issues with VOIP. Vendor representatives such as Bill Jensen, product marketing manager at Check Point, insist performance isn't an issue, even for his company's firewalls, which are software- rather than hardware-based. "On some of our appliances we're getting 3 Gbps of throughput," he said. "We can handle the throughput that's needed."

However, the issue may not be simply one of packet throughput and its effect on voice quality. Opening a port means updating the firewall's policy, and there isn't much of a time window in which to accomplish this. In a white paper, Dr. Andrew Molitor, chief scientist and co-founder of Aravox, noted that, in VOIP, voice packets follow very quickly on the heels of the control packets,

so "the firewall must be able to receive, install and acknowledge a policy change request in a matter of a few milliseconds" so that the port will be open when the voice packets start arriving.

And that's to make sure an *individual* call goes through. The firewall's processing must also be able to support enough simultaneous policy updates to handle the offered load of calls at the peak busy hour, Molitor added.

Organizational Issues

There are also non-technical issues. Just as the voice and data organizations within an enterprise must work together on VOIP implementations, there'll also need to be greater cooperation between those in charge of voice and those who specialize in network security. That won't necessarily be a smooth ride.

From the security manager's perspective, getting voice people involved in the details of firewall management could be uncomfortable, noted Check Point's Bill Jensen. "There's some trust issues there....You know security. The person doing voice over IP, who is often on the telco side of the business, doesn't necessarily have the depth of knowledge."

Likewise, Audin said the subject comes up in his training classes: "They're very chagrined, because they're mostly voice people, and they say: You mean I have to get involved with the security people for this? The answer is yes."

And when the subject is security, it's not necessarily a petty turf battle; enterprises with highly sensitive data want to keep everything relating to security on a need-to-know basis. "Here's an image for you," Audin said. "At Merrill Lynch, they got so paranoid that when they put in a firewall, they would tell the IP people to lay the cable on the floor; [the security staff] would come in at night and hook it up so you wouldn't even know who the

[security] people were."

Conclusion

Audin believes that VOIP firewalls haven't become a huge issue yet because of how companies are migrating toward VOIP: Many are either using private IP trunking for wide-area VOIP—"essentially a tie-line replacement between two PBXs"—or they're implementing only on the LAN side. In these scenarios, there's no VOIP traffic moving from an untrusted to a trusted network, and so firewall traversal doesn't become an issue.

"A lot of people have avoided it, just by not knowing they were avoiding it. They simply did one piece of VOIP, which essentially said firewalls weren't really necessary." Audin said. "The second or third stage of convergence really brings in the firewall problem."

Top of Page

BCR eWeekly :: BCR Magazine :: BCR Training :: CIO Boot Camp :: Collaboration Loop :: Collaborative Technologies Conference :: COMDEX :: GTEC Week :: Interop Las Vegas :: Interop New York :: Mobile Business Expo :: Mobility Loop :: NGN :: Seybold Bulletin :: Seybold Report :: VoiceCon Fall :: VoiceCon Spring :: VoiceCon eNews :: VoiceCon Tours :: VoIP Loop ::

CMP Media, LLC. | Legal | Privacy | Your California Privacy Rights | Mailing List | Contact Us

METHOD AND SYSTEM FOR FACILITATING SERVICES IN A COMMUNICATION NETWORK THROUGH DATA-PUBLICATION BY A SIGNALING SERVER

Patent number: WO03067363
Publication date: 2003-08-14
Inventor: MCCONNELL VON K (US); SANTHARAM ARUN (US)
Applicant: SPRINT SPECTRUM L P (US); MCCONNELL VON K (US); SANTHARAM ARUN (US)
Classification:
- international: ***H04L29/06;*** **H04L29/06;** (IPC1-7): G06F
- european: H04L12/28W; H04L12/56B; H04L29/06; H04L29/06C2
Application number: WO2002US36055 20021112
Priority number(s): US20020071833 20020207

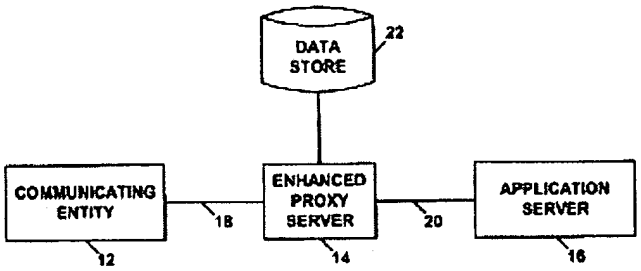
Also published as:
WO03067363 (A3)
US2003149774 (A1)
CA2472327 (A1)
AU2002360366 (A1)

Cited documents:
US2002147818
US2003021264

Report a data error here

Abstract of **WO03067363**

A mechanism is disclosed for facilitating the performance of communication services in a communication network. An enhanced proxy server receives a signaling message and proxies the message to an application server. Further, the enhanced proxy server responds to the message by extracting a set of data from a data store and making the set of data available for use by the application server in responding to the signaling message. Similarly, a registration server may receive a signaling message from a communicating entity and may responsively make data available for use by an application server in responding to signaling messages regarding the communicating entity.

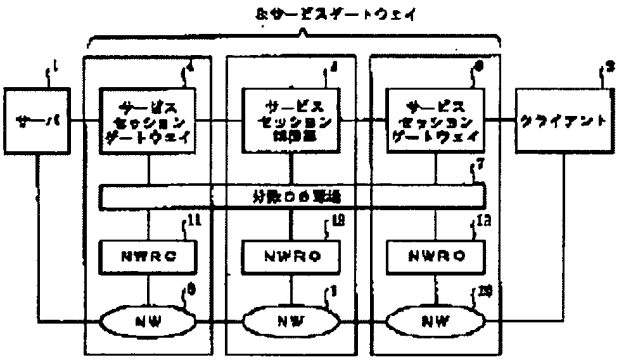


SERVICE SESSION CONTROLLER

Patent number: JP11065861
Publication date: 1999-03-09
Inventor: ISHIZUKA MASARU
Applicant: OKI ELECTRIC IND CO LTD
Classification:
- international: ***G06F9/46; G06F13/00; G06F15/16;*** **G06F9/46; G06F13/00; G06F15/16;** (IPC1-7): G06F9/46; G06F13/00; G06F15/16
- european:
Application number: JP19970236557 19970818
Priority number(s): JP19970236557 19970818

Abstract of **JP11065861**

PROBLEM TO BE SOLVED: To provide the device which performs service session control whatever decentralized OS environment a client is in. SOLUTION: Service session gateways 4 and 6 are provided between a server 1 and a session session control part 5, and a client 2 and the service session control part 5. If the client 2 is not initially in decentralized OS environment and the service session control part 5 performs control in decentralized OS environment, the service session gateway 6 converts a session control signal from the client 2 into a session control signal of the decentralized OS environment 7 based upon the decentralized environment.



70/9/7
DIALOG(R)File 256:TecInfoSource

00143275 DOCUMENT TYPE: Review

PRODUCT NAMES: Symantec Gateway Security (102881); UnityOne Network Defense System (120006); McAfee IntruShield (117617)

TITLE: Building the Perfect Box
AUTHOR: Walsh, Lawrence M
SOURCE: Information Security, v5 n10 p16(2) **Oct 2002**
ISSN: 1096-8903
HOMEPAGE: http://www.infosecuritymag.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Symantec's Symantec Gateway Security, TippingPoint's UnityOne, and IntruVert Networks' IntruShield are integrated appliances that combine multiple security measures. Vendors are beginning to combine **firewalls**, intrusion detection systems (IDSes), and other security technologies that can operate together. Low-end, all purpose devices, including Gateway Security Appliance, are an excellent choice for small- and mid-sized businesses (SMBs). Gateway Security Appliance and similar devices provide almost plug-and-play deployment and easy management, but do not have throughput, and their IDS signature databases are relatively small and non-changing. Integrated appliances such as UnityOne and IntruShield, provide protection against anomaly signature attacks by inspecting data packets for questionable attributes and behaviors and with the ability to automatically drop connections and **shut** down **ports**. With a single-component appliance, complexity and overhead are reduced, which reduces staffing requirements, but one drawback is easier hacking and cracking. Symantec also plans an enterprise-level version of Gateway, which uses technologies acquired with Riptech, SecurityFocus, MountainWave Technologies, and Recourse Technologies. UnityOne provides a **firewall**, IDS, and malware protection, but speed is up to 2Gbps. NetScreen Technologies has purchased OneSecure, and might add the latter technology to NetScreen's **firewall**/VPN offerings.

COMPANY NAME: Symantec Corp (386251); 3Com Corp (125105); McAfee Inc (490113)
SPECIAL FEATURE: Charts
DESCRIPTORS: Computer Security; **Firewalls**; Internetworking; Intrusion Detection; Network Administration; Network Software; System Monitoring
REVISION DATE: 20031030

7/9/2
DIALOG(R)File 2:INSPEC

08782068 INSPEC Abstract Number: B2003-12-8110C-035, C2003-12-6130S-057
Title: Application of OPSEC in network security management for power enterprises
Author(s): Huang Tianshu; Sun Fuxiong; Xiang Jidong; Yu Jingsong
Author Affiliation: Wuhan Univ., China
Journal: Automation of Electric Power Systems vol.27, no.13 p.54-7
Publisher: State Power Corp. of China,
Publication Date: 10 July 2003 Country of Publication: China
CODEN: DXZIE9 ISSN: 1000-1026
SICI: 1000-1026(20030710)27:13L.54:AONS;1-F
Material Identity Number: C804-2003-017
Language: Chinese Document Type: Journal Paper (JP)
Treatment: Applications (A)
Abstract: As a kind of commonly used product of network security, the network **firewall** is not capable of meeting all actual needs and special occasions of power enterprises. Then the users have to resort to other security software or develop it by themselves. Hence for the enterprise security system, the problem of how to integrate the new software with the current network security system into an organic whole is studied. Taking such commonly used hacker attack methods of DDOS, Trojan horses and **Port** -Scan as research objects, under the development environment of open platform for secure enterprise connectivity (OPSEC) and by use of the communal interface provided by OPSEC, a development practice is introduced, in which the designed security software for automatically detecting invasion and **alarming** is embedded in an OPSEC supporting enterprise **firewall** as an extensive **firewall** management module, together with the old **firewall** management module to defend hacker attacks. (5 Refs)

52/9/3
DIALOG(R)File 256:TecInfoSource

00149633 DOCUMENT TYPE: Review

PRODUCT NAMES: SecurVantage **Monitor** (151548

TITLE: EDS secures NMCI with Securify: Network **monitoring** tool helps...
AUTHOR: Jackson, Joab
SOURCE: Washington Technology, v18 n13 p25(1) **Sep 29, 2003**
ISSN: 1058-9163
HOMEPAGE: http://www.washingtontechnology.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

SecurVantage from Securify is a network security **monitoring** tool that automates the discovery of traffic that runs over a network. For systems with large numbers of applications **using** undocumented **ports**, SecurVantage is a fast and reliable method for establishing what the traffic pattern should be, and then **monitoring** network activity on **firewalls**, routers, authentication and authorization software, and so forth. If SecurVantage **detects** unusual activity, **it sends an alert**. Electronic Data Systems (EDS) uses SecurVantage to secure the Navy-Marine Corps Intranet, which uses more than 70,000 applications. SecurVantage provided EDS with the necessary traffic information, which **ports** and protocols the 70,000 applications use, so that EDS could secure this large network. After Navy policies were enforced, SecurVantage **monitored** for any unusual traffic. Other companies that provide network security **monitoring** tools include CyberGuard, Internet Security Systems, and Symantec.

COMPANY NAME: Securify Inc (692271)
SPECIAL FEATURE: Screen Layouts Tables
DESCRIPTORS: Computer Security; Government; Intranets; Network Administration; Network Software; System **Monitoring**

09/29/03; Vol. 18 No. 13

Tech Success: EDS secures NMCI with Securify

By JOAB JACKSON

Network monitoring tool helps identify many legacy applications

Electronic Data Systems Corp. in August awarded Securify Inc. a two-year, $5.8 million contract to help resolve a challenge the integrator had grappled with for almost three years: how to secure a huge network rife with legacy applications.

In October 2000, when EDS of Plano, Texas, won the eight-year, $6.9 billion contract to create the Navy-Marine Corps Intranet for more than 400,000 sailors and Marines, it faced the problem of integrating, at last count, more than 70,000 applications, according to Steve Vetter, a director of strategic planning for EDS.

For a network to run smoothly, the security team must know which ports and protocols the network applications use to communicate, so when viruses or unwanted visitors hit the network, they will be easily identified as errant. But with so many out-of-date and home-built applications running, many with unusual settings, making a list of what traffic was supposed to be on the network would be challenging.

"We've been wrestling with this problem. There are no silver bullets, but [Securify] was the closest thing we found," Vetter said.

Securify's SecurVantage security monitoring software can be used by integrators as well to help manage large networks, said Carl Wright, a former procurement officer for the Marines, and vice president of federal operations for Securify of Mountain View, Calif.

The field of network security monitoring tools is competitive, with contenders such as CyberGuard Corp., Internet Security Systems Inc. and Symantec Corp. Securify's competitive advantage is the wide breadth of network attributes that it monitors, Wright said. The software keeps tabs on everything from the host ports to whether someone is using an up-to-date public key infrastructure certificate.

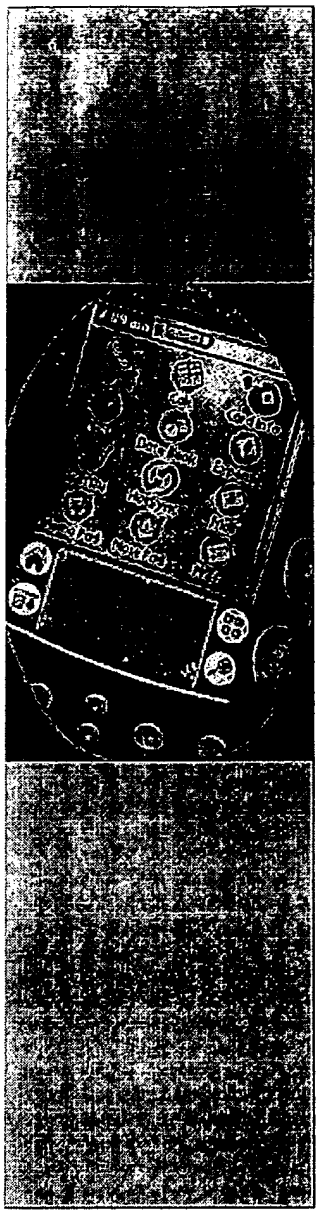
Installed at the boundaries between NMCI and other military networks, SecurVantage will help EDS and the Navy in two ways.

First, the Navy and EDS can automate discovering the types of traffic that usually run over network. On complex systems, this discovery process can be time-consuming. In many cases, the documentation for the Navy's legacy programs -- for those programs with documentation -- is not accurate.

"Many systems engineers made changes to applications, such as changing the ports used," and such changes were not updated in the documentation, Vetter said. Therefore, the only way EDS could determine how an application used a network would be to watch the behavior of that application in action.

SecurVantage can automatically characterize the traffic "flowing through" a network and give EDS officials a summary. EDS has begun to deploy it in this discovery process in selected Navy networks.

Once traffic is characterized and modified to conform to Navy standards, the software can monitor the network to watch for unusual activity. The software watches activity on firewalls, virus protection software, virtual private networks, routers and



authentication and authorization solutions.

If the traffic characteristics do not match what is authorized to go over that network, SecurVantage will alert EDS network administrators of the rogue communications. EDS, in turn, submits reports to the Navy's electronic warfare command.

With 50 employees, Securify was founded in 1998 as a consulting company, by ex-Netscape Corp. chief scientist Taher Elgamal. The company's product suite grew out of the tools the company developed internally to help financial institutions get a handle on the traffic flowing through their networks.

Today, government makes up about 80 percent of the private company's sales, with financial services accounting for most of the rest. The company does not divulge sales figures; however, research company Hoover's Inc., Austin, Texas, estimates Securify's 2002 sales at about $10 million.

Other government clients include the Defense Information Systems Agency, which uses Securify's products to secure command and control networks. In addition to the EDS deal, the Navy also uses Securify products for its own responsibilities in maintaining NMCI. Government-focused integrator partners include Artel Inc., Reston, Va., and Washington-based professional services company Centerprise Advisors Inc.

Integrators can use Securify to estimate more accurately how much work a potential contract could cost to implement, Wright said. The software can quickly build a characteristic of the traffic on that network, giving the integrator a clear picture of how much work will be needed to meet specifications. This information can help integrators estimate how much to bid for the work.

It also helps integrators merge networks. The NMCI project, for instance, involves combining many smaller office and base networks.

"What we do is help mitigate the complexity of large enterprise transitions by providing information based on real operational data," Wright said.

If you have an innovative solution that you recently installed in a government agency, contact Staff Writer Joab Jackson at jjackson@postnewsweektech.com.

Carl Wright is vice president of

(Image: David S. Spence)

Printer-Friendly Versi
Purchase A Reprint

ARCHIVES

Print edition

E-letters

EVENTS

Calendar

Submit your event

PostNewsweek Awards

ONLINE RESOURCES

Upcoming online forums

Forum transcripts

Resource Centers

XML Feeds

COMPANY RANKINGS

Marketplace

Products and services from our sponsors

Top 100 Federal Prime Contractors

Small Business / 8(a)

Fast 50

State & Local Who's Who

M & A Report

Top 100 Political Contributions

COMPANY PROFILES

Tech Almanac

SPONSORED SOLUTIONS

Index of technology reports

Product/Services Finder

WASHINGTON TECHNOLOGY

Site Map
About Washington Technology
Customer Help
Editorial Calender
Advertising
Subscriptions
Link Policy / Reprints
Privacy Policy
Careers

Publishing Systems
Powered By

14/9/6
DIALOG(R)File 2:INSPEC

08474257 INSPEC Abstract Number: B2003-01-6210L-165, C2003-01-5620W-102
Title: Transport layer proxy for stateful UDP packet filtering
Author(s): Chang, R.K.C.; Fung, K.P.
Author Affiliation: Dept. of Comput., Hong Kong Polytech. Univ., Kowloon, China
Conference Title: Proceedings ISCC 2002 Seventh International Symposium on Computers and Communications p.595-600
Editor(s): Corradi, A.; Daneshmand, M.
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 2002 Country of Publication: USA xxiv+1051 pp.
ISBN: 0 7695 1671 8 Material Identity Number: XX-2002-02138
U.S. Copyright Clearance Center Code: 0-7695-1671-8/02/$17.00
Conference Title: Proceedings ISCC 2002 Seventh International Symposium on Computers and Communications
Conference Sponsor: IEEE Commun. Soc.; IEEE Comput. Soc
Conference Date: 1-4 July 2002 Conference Location: Taormina-Giardini Naxos, Italy
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: **Firewall** support for UDP traffic today is still insecure and inadequate. We propose in this paper a transport layer proxy (TLP) to provide a secure UDP **firewall** traversal service on the transport layer (the TLP supports TCP as well). For each UDP association with endpoints separated by a TLP server, the TLP server performs user-level or host-level authentication, packet filtering, packet relaying, optional network address translation, session logging, **timing**-out of idle association, and other security-related functions. The core of the TLP is a two-step TLP binding procedure that makes a UDP association stateful between a TLP client and a TLP server. This binding procedure supports Active UDP Open, Passive UDP Open, and Source-Specific UDP Open, which a local program may perform on a UDP socket. (7 Refs)
Subfile: B C
Descriptors: authorisation; client-server systems; Internet; packet switching; protocols; telecommunication security
Identifiers: transport layer proxy; stateful UDP packet filtering; **Firewall** support; UDP traffic; TLP; secure UDP **firewall** traversal service; user-level authentication; host-level authentication; packet filtering; packet relaying; optional network address translation; session logging; **timing**-out; idle association; security-related functions; two-step TLP binding procedure; TLP client; TLP server; Active UDP Open; Passive UDP Open; Source-Specific UDP Open; UDP socket
Class Codes: B6210L (Computer communications); B6150C (Communication switching); B6150M (Protocols); C5620W (Other computer networks); C6130S (Data security); C5640 (Protocols)

14/9/10
DIALOG(R)File 2:INSPEC

06175411 INSPEC Abstract Number: B9603-6150C-026, C9603-1140C-016
Title: Delay guarantee of virtual clock server
Author(s): Xie, G.G.; Lam, S.S.
Author Affiliation: Dept. of Comput. Sci., Texas Univ., Austin, TX, USA
Journal: IEEE/ACM Transactions on Networking vol.3, no.6 p.683-9
Publisher: IEEE,
Publication Date: Dec. 1995 Country of Publication: USA
CODEN: IEANEP ISSN: 1063-6692
SICI: 1063-6692(199512)3:6L.683:DGVC;1-8
Material Identity Number: P946-96001
U.S. Copyright Clearance Center Code: 1063-6692/95/$04.00
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: In a packet switching network, **each communication channel** is statistically shared among many traffic flows that belong to different end-to-end sessions. We present and prove a **delay** guarantee for the virtual clock service discipline (inspired by time division multiplexing). The guarantee has several desirable properties, including the following **firewall** property: the guarantee to a flow is unaffected by the behavior of other flows sharing the same server. There is no assumption that sources are flow controlled or well behaved. We first introduce and define the concept of an active flow. The delay guarantee is then formally stated as a theorem. We show how to obtain delay bounds from the delay guarantee of a single server for different specifications. (15 Refs)
Subfile: B C
Descriptors: **clocks**; delays; network servers; packet switching; queueing theory; switching networks; telecommunication congestion control; telecommunication networks; telecommunication traffic
Identifiers: virtual clock server; delay guarantee; **firewall** property; active flow; flow control; delay bounds; communication channel; packet switching networks; virtual clock service discipline; time division multiplexing; TDM; FCFS; queueing theory; packet switching; communication traffic
Class Codes: B6150C (Communication switching); B0240C (Queueing theory); B6150J (Queueing systems); C1140C (Queueing theory); C3370 (Control applications in telecommunications)

22/9/5
DIALOG(R)File 2:INSPEC

08956755 INSPEC Abstract Number: B2004-06-6210D-011, C2004-06-5620W-115
Title: The border patrol: **firewalls** for VOIP
Author(s): Audin, G.
Journal: Business Communications Review vol.33, no.10 p.23-7
Publisher: BCR Enterprises,
Publication Date: Oct. 2003 Country of Publication: USA
CODEN: BCORBD ISSN: 0162-3885
SICI: 0162-3885(200310)33:10L.23:BPFV;1-O
Material Identity Number: F939-2003-010
U.S. Copyright Clearance Center Code: 0162-3885/2003/$0.00+.50
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: **Firewalls** provide security by blocking intrusions into an enterprise network. But **firewalls** also produce performance problems and cause **delay**. Most **firewalls** are designed for data applications and are not application specific, though some **firewall** vendors (such as Checkpoint, Jasomi, Datapower, F5 and Sarvega) are moving toward packet content analysis (called deep packet inspection). This is a move to more application-specific security, though even it does not yet cover voice over IP (VOIP) packet analysis. VOIP traffic requires real-time delivery, short **delay** , low jitter and low packet loss across networks. Data **firewalls** are not designed for real-time applications. Among other issues, they have difficulty dealing with network address translation (NAT) and VOIP signaling. A VOIP call uses either the TCP or UDP protocol with well-known application **ports** to set up a call. To deal with these issues, a few vendors have created a new class of product, the real-time firewall (RTF), specifically designed to handle both data and real-time applications like voice and video over IP. The significant difference between data and real-time firewalls is their performance for video traffic. For many enterprises, the solution may be a separate application-specific real-time firewall (RTF) running in parallel to the existing data firewall , a hardware-rather than software-based devices. In this way, the VOIP traffic passes through a firewall specifically designed for its needs, while blocking data traffic. At the same time, the data firewall blocks VOIP signaling and traffic without penalizing the VOIP traffic.
Subfile: B C
Descriptors: authorisation; business communication; Internet telephony; IP networks; telecommunication traffic; transport protocols
Identifiers: Internet Protocol; voice over IP **firewall**; intrusion blocking; enterprise network; **delay**; real-time application; low packet loss; low jitter; data **firewall**; user datagram protocol; UDP; Transport Control Protocol; TCP protocol; application **port**; application-specific real-time **firewall**; data application; video over IP; video traffic; voice over IP traffic; data traffic blocking; network address translation; voice over IP signaling
Class Codes: B6210D (Telephony); B6210L (Computer communications); B6150M (Protocols); C5620W (Other computer networks); C6130S (Data security); C5640 (Protocols)

7/9/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016327233 **Image available**
WPI Acc No: 2004-485130/200446
XRPX Acc No: N04-382774
Firewall notifies changed **port** number to carry out access permit to client, when **port** number carrying out access permit is not matched with stored identification number of client
Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 2004192044	A	20040708	JP 2002355614	A	20021206	200446 B

Priority Applications (No Type Date): JP 2002355614 A 20021206
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2004192044	A		12	G06F-013/00	

Abstract (Basic): JP 2004192044 A
NOVELTY - A **port** monitoring processor (11) stores the identification (ID) number of client as access permit **port** number. When the **port monitoring** processor with a filter processor (13) determines that access situation of the **port** number carrying out the access is not matched with the stored ID number of the client, an access controller (14) changes the **port** number and **notifies** to the client (2) and server (3).
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(1) server;
(2) firewall system; and
(3) recorded medium storing the **port** number change program.
USE - Firewall for interrupting irregular access from the outside with respect to network system such as internet.
ADVANTAGE - The security level of the firewall is improved.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the firewall system. (Drawing includes non-English language text).
firewall (1)
client (2)
server (3)
port monitoring processor (11)
port management table (12)
filter processor (13)
access controller (14)
pp; 12 DwgNo 9/9
Title Terms: FIREWALL; **NOTIFICATION**; CHANGE; **PORT**; NUMBER; CARRY; ACCESS; PERMIT; CLIENT; **PORT**; NUMBER; CARRY; ACCESS; PERMIT; MATCH; STORAGE; IDENTIFY; NUMBER; CLIENT
Derwent Class: T01; W01
International Patent Class (Main): G06F-013/00
International Patent Class (Additional): G06F-012/00; G06F-012/14; G06F-015/00; H04L-012/66
File Segment: EPI
Manual Codes (EPI/S-X): T01-H; T01-H01C2; T01-J; T01-S03; W01-A06G3

7/9/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014180644 **Image available**
WPI Acc No: 2002-001341/200201
Related WPI Acc No: 2001-572988; 2001-591651; 2001-597165; 2001-597166; 2001-598742
XRPX Acc No: N02-000996
Method and machine for configuring **firewalls** in a computer data system
Patent Assignee: BULL SA (SELA)
Inventor: FAVIER V; GRARDEL F; GUIONNEAU C

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2806812	**A1**	**20010928**	**FR 9916121**	**A**	**19991221**	**200201**	**B**

Priority Applications (No Type Date): FR 9916121 A 19991221
Abstract (Basic): FR 2806812 A1

NOVELTY - Method of configuring a firewall (2) in a data system (3) having objects (4). An access control protocol is put in place for the objects being called by resources (13). Switching, for communication with the system, is controlled by imposing one or more network interfaces required for the passage of a communication between an origin resource and a destination resource.

DETAILED DESCRIPTION - Access to firewall protected zones (5) is not allowed to interfaces being used whilst the communication process is being done. Extended ownership services are used to allow the addition of supplementary switching application criteria. These criteria, as a function of which communication passage is imposed, are the calling address, the called address, the application called, the calling user, an authentication type, an application period (time and date of access), use level and/or an **alert** caused by a particular action associated with a particulate event.

An Independent Claim is included for - A firewall configuration machine.

USE - For access control to computer data systems

ADVANTAGE - Designed to allow a firewall administrator to control the switching of data packets at firewall level as a function of various criteria such as source address and/or **port** numbers, for a user who requests access at a particular time and date.

DESCRIPTION OF DRAWING(S) - The drawings shows a schematic of the firewall and system

configuration machine (1)
firewall (2)
data system (3)
objects (4)
firewall protected zones (5)
internal sub-network (6)
demilitarized sub network (7)
internet sub network (8)
liaison sub network for firewalls (9)
interfaces (10)
firewall configuration machine (11)
administrator (12)
resources (13)
graphical interface (14)
compilation driver (15)
tele-loading module (16)

7/9/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013499930 **Image available**
WPI Acc No: 2000-671871/200065
Related WPI Acc No: 1999-458217; 2000-282810; 2000-490547; 2000-585979; 2001-023206; 2002-105000; 2002-170856; 2004-830853
XRPX Acc No: N00-498038

Firewall server service quality managing method used in internet, involves estimating bit rate over round trip time between source and receiver, based on which acknowledgment signal is transmitted or **delayed**

Patent Assignee: UKIAH SOFTWARE INC (UKIA-N)
Inventor: SAWHNEY S; VAID A
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6119235	**A**	**20000912**	**US 9747752**	**P**	**19970527**	**200065 B**
			US 97998332	A	19971224	

Priority Applications (No Type Date): US 9747752 P 19970527; US 97998332 A 19971224
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6119235	A		14	G06F-011/30	Provisional application US 9747752

Abstract (Basic): US 6119235 A

NOVELTY - The data source and receiver connection is classified into a traffic class. Bit rate over a round trip time between the source and the receiver is determined. The firewall server transmits and delays the acknowledgment signal to the source, when the bit rate is less than and exceeds the bit rate limit, respectively.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) firewall server;
(b) computer program product;
(c) method for managing network traffic via a network

USE - Used for manipulating and allocating bandwidth on a telecommunication network like internet, local area network, wide area network etc.

ADVANTAGE - The telecommunication traffic including directory service and bandwidth management is managed at a single region that is the firewall server. The implementation into a pre-existing system, is relatively easy as the quality management method is predominantly software base which can be easily installed to the existing system.

DESCRIPTION OF DRAWING(S) - The figure shows a simplified block diagram of a flowchart for the firewall server service quality managing method.

pp; 14 DwgNo 5/7

Title Terms: FIREWALL; SERVE; SERVICE; QUALITY; MANAGE; METHOD; ESTIMATE; BIT; RATE; ROUND; TRIP; TIME; SOURCE; RECEIVE; BASED; SIGNAL; TRANSMIT; DELAY
Derwent Class: T01
International Patent Class (Main): G06F-011/30
File Segment: EPI

22/9/7
DIALOG(R)File 2:INSPEC

08765295 INSPEC Abstract Number: B2003-12-6210L-016, C2003-12-5620-001
Title: Intrusion prevention systems: security's silver bullet?
Author(s): Sequeira, D.
Journal: Business Communications Review vol.33, no.3 p.36-41
Publisher: BCR Enterprises,
Publication Date: March 2003 Country of Publication: USA
CODEN: BCORBD ISSN: 0162-3885
SICI: 0162-3885(200303)33:3L.36:IPSS;1-D
Material Identity Number: F939-2003-005
U.S. Copyright Clearance Center Code: 0162-3885/03/$0.50
Language: English Document Type: Journal Paper (JP)
Treatment: General, Review (G)
Abstract: Traditionally, **firewalls** and anti-virus programs try to block attacks, and intrusion detection systems (IDSs) identify attacks as they occur. Such techniques are crucial to network security, but have limitations. A **firewall** can stop attacks by blocking certain **port** numbers, but it does little to analyze traffic that uses allowed **port** numbers. IDSs can monitor and analyze traffic that passes through **open ports** , but do not prevent attacks. With the proliferation of sophisticated attacks and the discovery of new vulnerabilities, new methods are needed to protect precious data and network resources. Intrusion prevention systems (IPSs) use new proactive approaches that block attacks before damage is done. The article looks at the different approaches taken by IDSs and IPSs, including host-based IPS (HIPS) and network-based IPS (NIPS). **Firewalls**, antivirus, IDS and IPS have their place in the security landscape, each with its unique features, and are not competing components. Bulletproof security does not exist. Security is a continuous process of **monitoring**, maintenance and modification, and no amount of automation can replace trained and vigilant personnel. Tools like IPS can provide a silver lining if not a silver bullet.
Subfile: B C
Descriptors: authorisation; computer network management; computer viruses ; telecommunication security
Identifiers: intrusion prevention systems; network security; **firewalls**; anti-virus programs; intrusion detection systems; IDS; traffic; proactive approach; host-based IPS; network-based IPS
Class Codes: B6210L (Computer communications); B6210C (Network management); C5620 (Computer networks and techniques); C6130S (Data security)

22/9/8
DIALOG(R)File 2:INSPEC

08705374 INSPEC Abstract Number: B2003-09-6210D-003
Title: **Firewalls** face next-gen challenges
Author(s): Krapf, E.
Journal: Business Communications Review vol.33, no.4 p.55-8
Publisher: BCR Enterprises,
Publication Date: April 2003 Country of Publication: USA
CODEN: BCORBD ISSN: 0162-3885
SICI: 0162-3885(200304)33:4L.55:FFNC;1-N
Material Identity Number: F939-2003-003
U.S. Copyright Clearance Center Code: 0162-3885/03/$0.00+.50
Language: English Document Type: Journal Paper (JP)
Treatment: General, Review (G)
Abstract: VOIP poses two main challenges for **firewalls**: the need to deal with network address translation (NAT), and the need to **open** lots of **firewall ports** to let VOIP through. A group of companies is taking on the challenge, each with its own solution.
Subfile: B
Descriptors: authorisation; business communication; Internet telephony; protocols
Identifiers: VOIP; network address translation; NAT; **firewall ports**; enterprise managers
Class Codes: B6210D (Telephony); B6210L (Computer communications); B6150M (Protocols)

22/9/9
DIALOG(R)File 2:INSPEC

08290485 INSPEC Abstract Number: C2002-07-5620-022
Title: An intelligent agent security intrusion system
Author(s): Pikoulas, J.; Buchanan, W.; Mannion, M.; Triantafyllopoulos, K.
Author Affiliation: Napier Univ. of Edinburgh, UK
Conference Title: Proceedings Ninth Annual IEEE International Conference and Workshop on the Engineering of Computer-Based Systems p.94-9
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 2002 Country of Publication: USA x+277 pp.
ISBN: 0 7695 1549 5 Material Identity Number: XX-2002-01093
U.S. Copyright Clearance Center Code: 0-7695-1549-5/02/$17.00
Conference Title: Proceedings Ninth Annual IEEE International Conference and Workshop on the Engineering of Computer-Based Systems
Conference Sponsor: IEEE Comput. Soc. Tech. Committee on Eng. of Comput.-Based Syst
Conference Date: 8-11 April 2002 Conference Location: Lund, Sweden
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Experimental (X)
Abstract: Network security has now become one of the most important aspects in computer systems and the Internet. Apart from strong encryption, there is no definite method of truly securing network, thus they must be protected at different levels of the OSI model. At the physical layer, they can be protected by lock-and-key, and at the data link, they can be protected within VLANS (virtual LANs). With the network and transport layers, networks can be secured by **firewalls**, which **monitor** source and destination network addresses, and source and **destination ports**, respectively. At the session level, user names and passwords are be used. Unfortunately, all these methods can be prone to methods which can overcome the protection used. This paper expands the research previously undertaken on a misuse system based on the intelligent agent software technology. The system monitors user actions in real-time and take appropriate actions if necessary. Along with this our system uses a short-term prediction to predict the user behaviour and advises the system administrator accordingly, before the actual actions take place. This paper presents new results, which are based on an increased number of users. We tested our short-term prediction model, introduced the notion of intervention to our model, and found that the results are very **close** to the actual user behaviour. (2 Refs)
Subfile: C
Descriptors: computer network management; computerised **monitoring**; real-time systems; security of data; software agents
Identifiers: intelligent agents; security intrusion system; computer network security; encryption; network protection; user actions **monitoring**; real-time systems; short-term prediction; user behaviour prediction
Class Codes: C5620 (Computer networks and techniques); C6130S (Data security); C6170 (Expert systems and other AI software and techniques)

22/9/10
DIALOG(R)File 2:INSPEC

08114163 INSPEC Abstract Number: B2002-01-6210L-218, C2002-01-5620-052
Title: Detection and protection against network scanning: IEDP
Author(s): Guo Xiaobing; Qian Depei; Liu Min; Zhang Ran; Xu Bin
Author Affiliation: Dept. of Comput. Sci. & Eng., Xi'an Jiaotong Univ., China
Conference Title: Proceedings 2001 International Conference on Computer Networks and Mobile Computing p.487-93
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 2001 Country of Publication: USA xii+529 pp.
ISBN: 0 7695 1381 6 Material Identity Number: XX-2001-02358
U.S. Copyright Clearance Center Code: 0-7695-1381-6/01/$10.00
Conference Title: Proceedings 2001 International Conference on Computer Networks and Mobile Computing
Conference Sponsor: China Comput. Federation.; IEEE Comput. Soc., Beijing Center; IEEE Comput. Soc. Tech. Committee on Distributed Process
Conference Date: 16-19 Oct. 2001 Conference Location: Los Alamitos, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Network scanning is an increasing threat to network security. This paper classifies and analyzes current scanning methods, and draws a conclusion that the current detection and protection of scanning mainly aim at information concealment. A novel system of the detection and protection named IEDP is presented in this paper Its concept is discussed and its implementation is described in details. Compared with the current approaches, the concept of IEDP can be recapitulated in one word: "impartation". When detecting a scanning, IEDP gives the scanner bogus information to spoof and confuse him/her. So, for example, when scanning **ports**, the scanner will find that all **ports** are listening and can't tell which **port** is really **open**. IEDP also adopts a new mechanism called error steering to spoof the scanner IEDP randomly steers errors in communication with the scanner, let the scanner believe that the communication is unstable and give up scanning. Experiments show that IEDP system is efficient. (8 Refs)
Subfile: B C
Descriptors: computer networks; security of data; telecommunication security
Identifiers: network scanning; network attack; network security; IEDP system; **firewall**; protection; detection
Class Codes: B6210L (Computer communications); C5620 (Computer networks and techniques); C6130S (Data security)

22/9/15
DIALOG(R)File 2:INSPEC

06768052 INSPEC Abstract Number: B9801-6210L-127, C9801-6130S-034
Title: **Firewall** placement in a large network topology
Author(s): Smith, R.N.; Bhattacharya, S.
Author Affiliation: Dept. of Comput. Sci. & Eng., Arizona State Univ., Tempe, AZ, USA
Conference Title: Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems (Cat. No.97TB100190) p.40-5
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 1997 Country of Publication: USA xii+346 pp.
ISBN: 0 8186 8153 5 Material Identity Number: XX97-02929
U.S. Copyright Clearance Center Code: 1071-0485/97/$10.00
Conference Title: Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems
Conference Sponsor: IEEE Comput. Soc. Tech. Committee on Distributed Process
Conference Date: 29-31 Oct. 1997 Conference Location: Tunis, Tunisia
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Network security is an integral component of a multi-user distributed information environment. **Firewall** (FW) technology is a popular approach to build secure networks, and a plethora of FWs have been designed. Our research focuses on the placement of FWs (i.e. an operations research approach) in a large, complex network system, or a system of systems. A key contribution of this research is to propose the concept of a FW cascade, i.e. a chain of FWs, which could be placed in the path between a potential attack point and a network node with sensitive data. Among other benefits, the FW cascade offers two key benefits: (1) increased comprehensiveness (viz. address, **port** , service, user ID and direction) of security protection; and (2) most importantly, enhancing the degree of confidence that the network security engineer could expect from the underlying set of FWs and the overall end-to-end security protection that is achieved. This results in a novel capability, where a network security engineer can provide completeness and high confidence in the security attributes across the network. We propose a decomposition of the security characters of a FW and a suite of FW placement heuristics which allows us to place the FWs across the network while optimizing cost and maximizing security protection. Minimization of **delay** is another optimization goal. Performance is depicted using simulation. (5 Refs)
Subfile: B C
Descriptors: authorisation; **delays**; internetworking; network topology; operations research; optimisation; performance evaluation; wide area networks
Identifiers: **firewall** placement heuristics; large network topology; network security; multi-user distributed information environment; operations research; **firewall** cascade; potential attack point; sensitive data; comprehensive security protection; confidence degree; end-to-end security protection; completeness; cost optimization; **delay** minimization; performance; simulation
Class Codes: B6210L (Computer communications); C6130S (Data security); C1180 (Optimisation techniques); C5670 (Network performance); C5620W (Other computer networks)